



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/764,541	01/17/2001	John R. Hind	RSW920010013US1	6481
25259	7590	10/05/2004		
IBM CORPORATION 3039 CORNWALLIS RD. DEPT. T81 / B503, PO BOX 12195 REASEARCH TRIANGLE PARK, NC 27709			EXAMINER STULBERGER, CAS P	
			ART UNIT	PAPER NUMBER
			2132	

DATE MAILED: 10/05/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/764,541

Applicant(s)

HIND ET AL.

Examiner

Cas Stulberger

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-38 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-38 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 17 January 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**BEST AVAILABLE COPY****Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_.

**DETAILED ACTION**

***Claim Rejections - 35 USC § 103***

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,009,176 to Gennaro et al., in view of U.S. Patent No. 5,666,415 to Kaufman, and in further view of 5,923,763 to Walker et al.

3. In regards to claims 1-3, 6-15, 18-27, and 30-38, Gennaro discloses a method of signing digital streams. Gennaro discloses splits the streams into blocks and creates a table listing cryptographic hashes of each of the blocks (Gennaro: column 1, lines 23-27). This meets the limitation of "computer-readable program code means for computing a hash value over each of the plurality of data streams, wherein each data stream is created by a different application processing component." The sender then signs the table (Gennaro: column 1, lines 26-27). This meets the limitation of "computer-readable program code means for digitally signing the hashed combination data block with a private cryptographic key, wherein the private cryptographic key and a public cryptographic key which is cryptographically associated therewith represent a digital notary." Gennaro however does not disclose "computer-readable program code means for combining each hash value with a unique identifier of the application processing component which created the data stream for which the hash value was computed, thereby creating a

combination data block; computer-readable program code means for hashing the combination data-block.”

4. Walker discloses a unique device identification number stored in RAM or memory can be added to the hash (Walker: column 5, lines 54-55). This meets the limitation of “computer-readable program code means for combining each hash value with a unique identifier of the application processing component which created the data stream for which the hash value was computed, thereby creating a combination data block.”

5. It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method of hashing and signing digital streams as disclosed by Gennaro with the method of adding a unique device identification number to the hash in order to provide assurance of message authenticity (Walker: column 5, line 56).

6. However neither Gennaro nor Walker disclose “computer-readable program code means for hashing the combination data-block.” Kaufman discloses the “Lamport Hash” scheme where a password is iteratively transforms a password multiple times (Kaufman: column 3, lines 21-27).

7. It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method of hashing and signing digital streams as disclosed by Gennaro with the method of hashing the combination of the hash and unique identification number as disclosed by Kaufman in order to prevent against eavesdropping (Kaufman: column 3, line 31).

Art Unit: 2132

8. In regards to claim 4, 16, and 28, Gennaro discloses MPEG (Gennaro: column 1, line 37).

9. In regards to claims 5, 17, and 29, Gennaro discloses that each block can be verified when it arrives (Gennaro: column 1, lines 32-33).

*Conclusion*

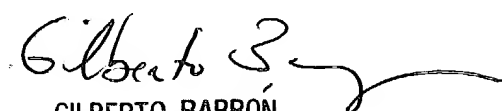
10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Cas Stulberger whose telephone number is (703) 305-8034. The examiner can normally be reached on Monday - Friday, 9:00A.M. - 5:00P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CS

CS

  
GILBERTO BARRON  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

BEST AVAILABLE COPY